DEFENCE R&D DÉFENSE

Multi-Modal Biometric Approaches to Anti-Spoofing

Qinghan Xiao

Defence R&D Canada - Ottawa

March 31, 2005

Outline

- Authentication vs. E-Authentication
  - Locally controlled environment
  - Remotely open environment
- Spoofing
  - Steal a biometric sample
  - Create a fake artefact
- Anti-Spoofing
  - Liveness detection
  - Multi-modal biometric fusion

User Authentication

Authentication can be divided into four categories

- Local
  - supervised
  - unsupervised
- Remote
  - supervised
  - unsupervised

Local Authentication

- Authentication performed within a small group
  - Each user has a relatively fixed access point
- Authentication located in the trusted environment
  - Locally in an office environment
  - LAN access is controlled

E-Authentication

- E-authentication is the key to success e-government.
  - Ensure that the government transacts business with the right person
  - Allow users to trust the security of the information provided
  - Reassure users that their privacy will be protected
- New Challenge
  - Authenticate the users from remote locations
  - Network is opened to every one

Authentication Factors

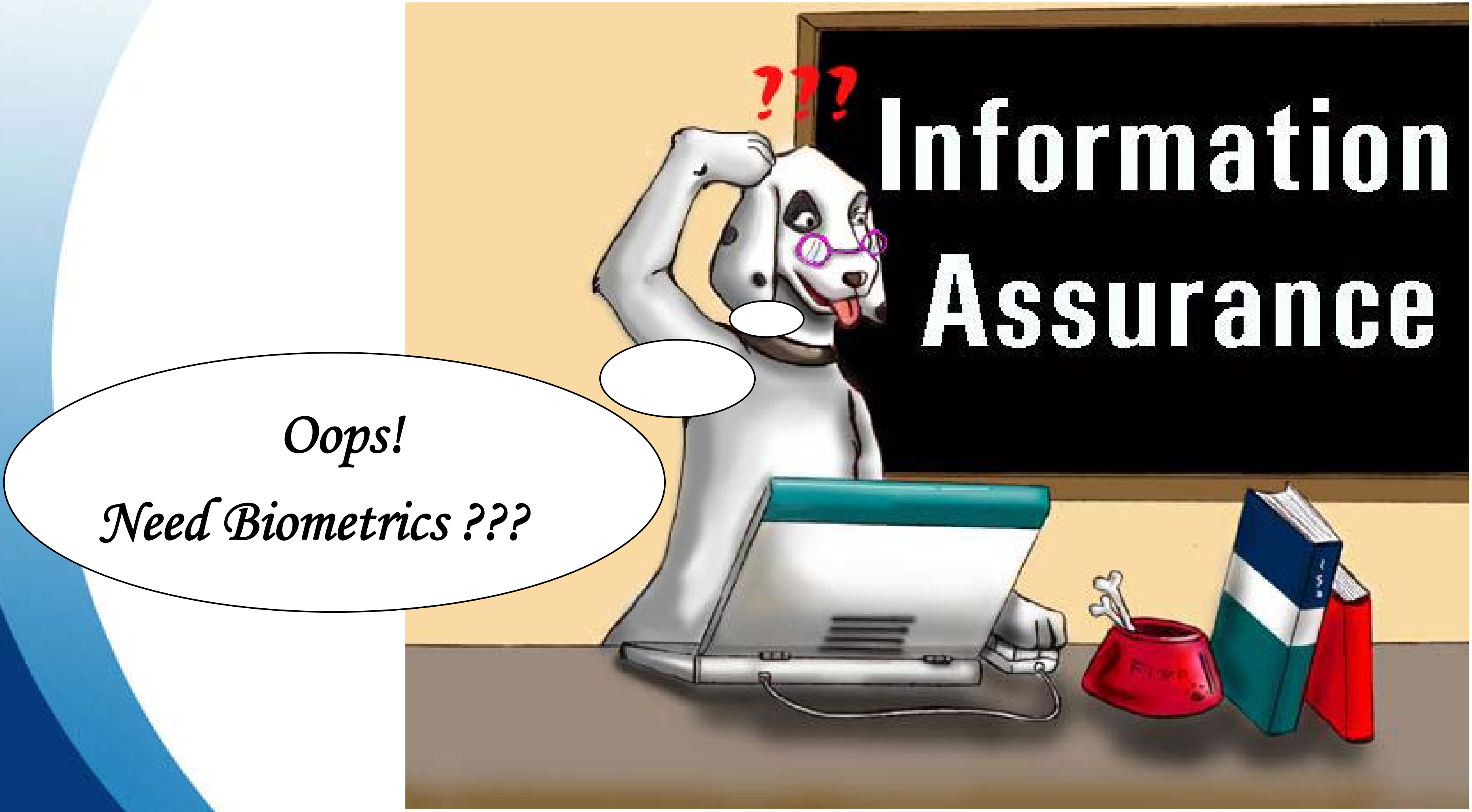
Security Level
Solutions

Any technology can be broken by some one, in some way, at some time, with some efforts.

Authentication without Biometrics

If I know the password
no one knows I am a dog!
Information
Assurance

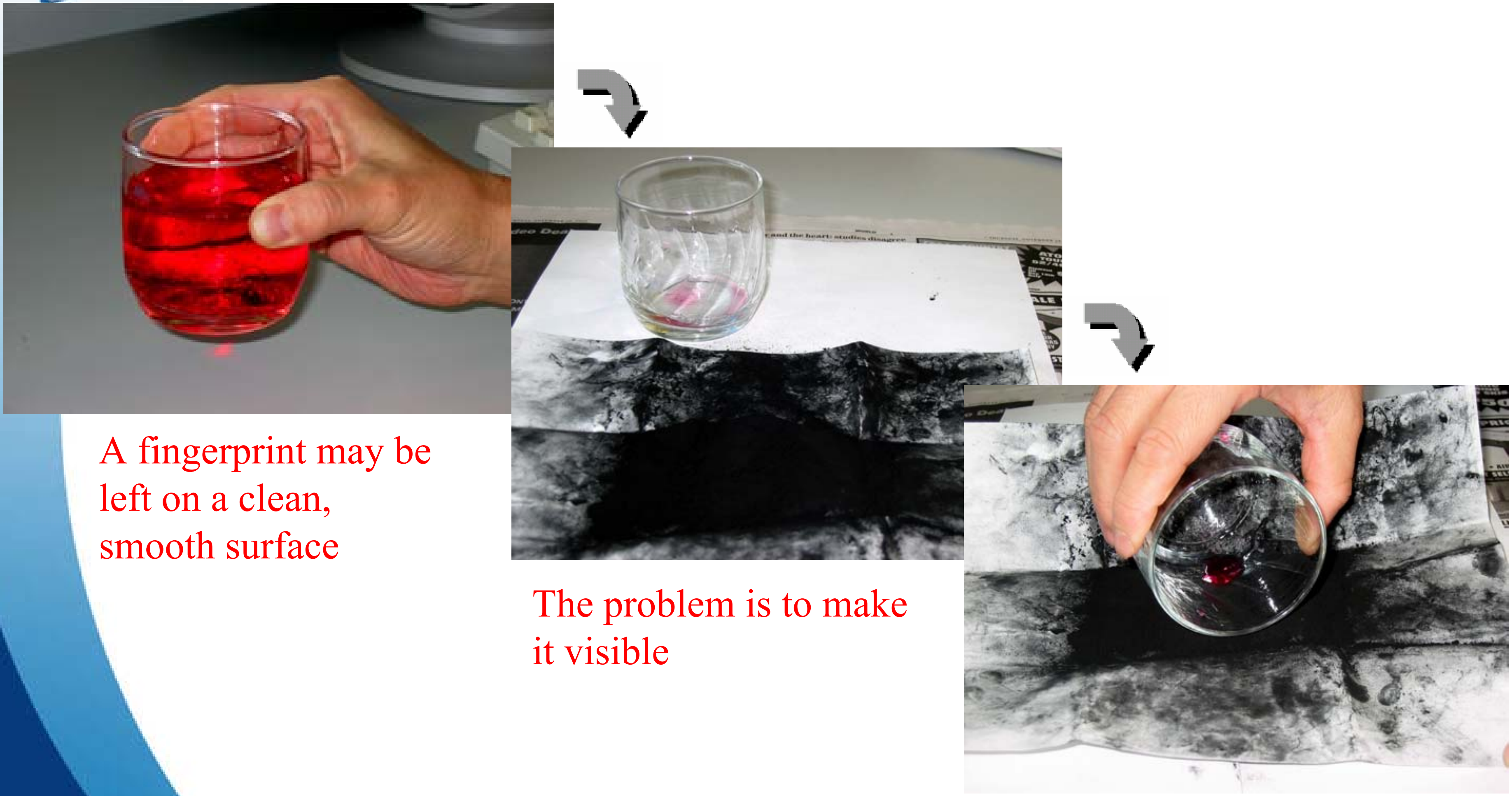
Authentication with Biometrics



Spoofing Problem

- Fingerprint sensor can be attacked by
  - Recovering latent fingerprint from sensor window,
  - Using residual prints
  - Creating fake fingers with gelatine or silicon rubber to fool the sensor
- Face Recognition can be attacked by
  - Stealing face photo
  - Recording facial video
  - Creating 3D face mask

Spoofing: Easy to still a biometric sample

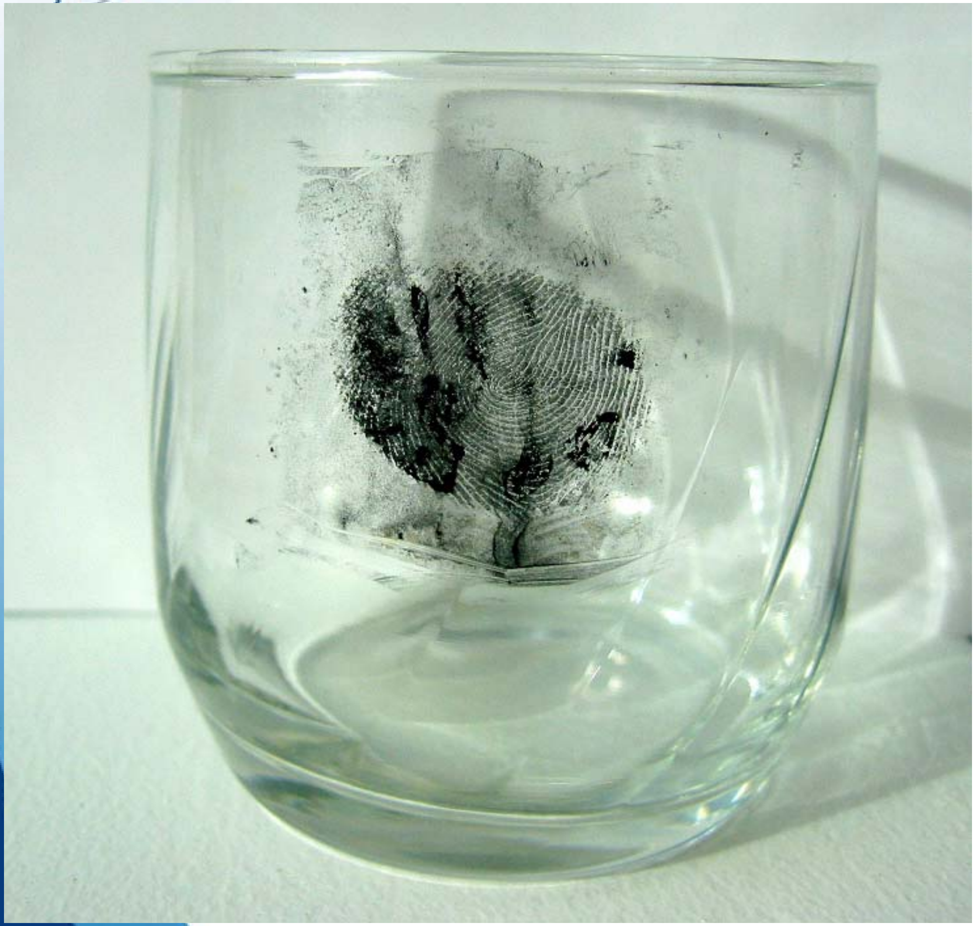


A fingerprint may be left on a clean, smooth surface

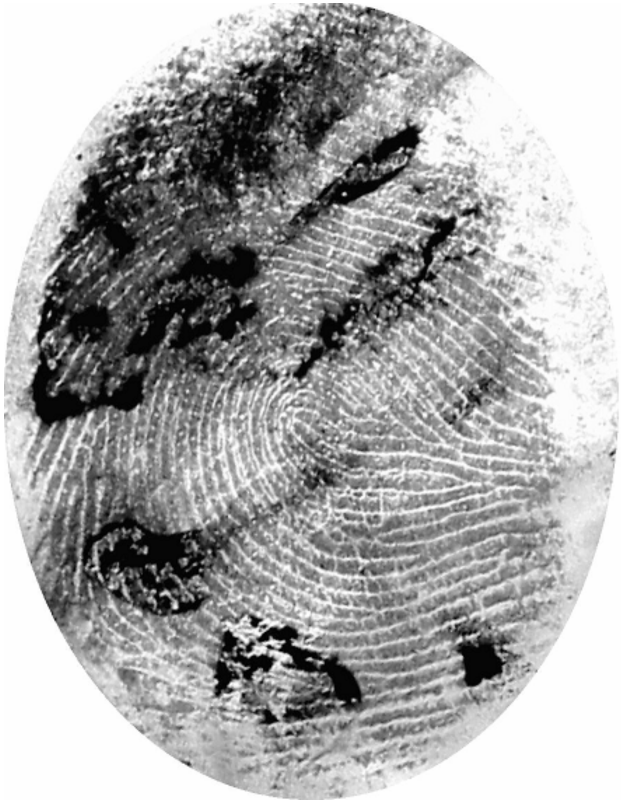
The problem is to make it visible

Black toner is cheap and can be used to get the fingerprint

Fingerprint Image Captured



There it is!!!



A digital camera can be used to take the fingerprint image. The image can then be edited by image processing software…

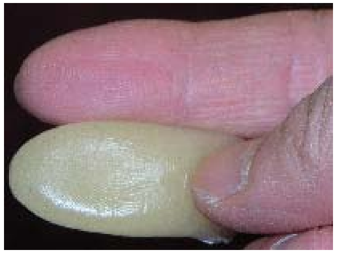
Spoofing: Easy to create an artefact

Use cheap materials to fool fingerprint sensor

Press live finger against free molding plastic

Get a mold

Pour the liquid into the mold



The gummy finger

Attack fingerprint sensor

Matsumoto's technique [1]

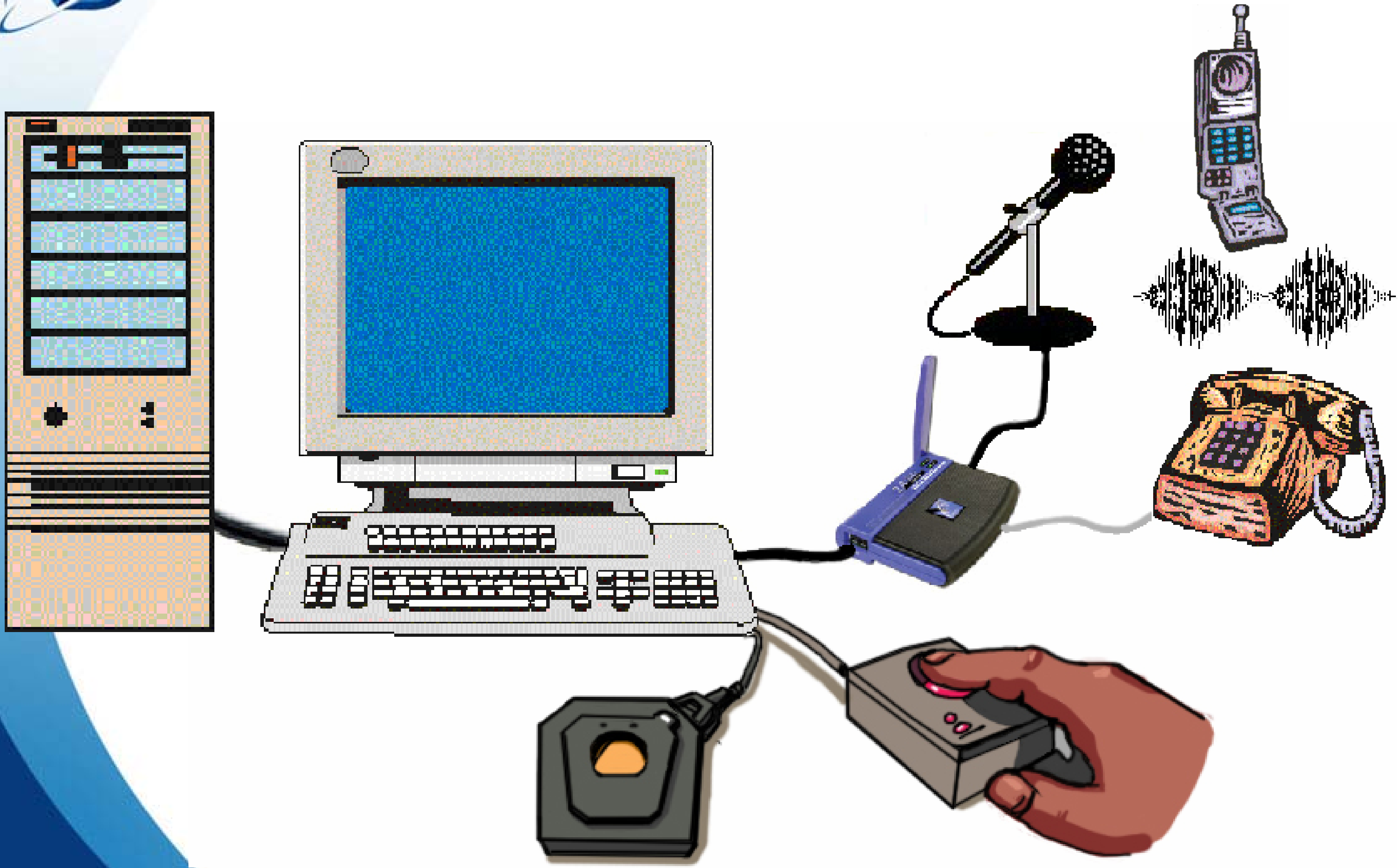
Anti-Spoofing Techniques

- Liveness Detection
  - Fingerprint
    - Temperature, Heartbeat, Finger bone
    - LightPrint
  - Face
    - Eye blink
    - Fourier spectra analysis
- Multi-Modal Biometrics

DRDC’s Research on Multi-Modal Biometric System

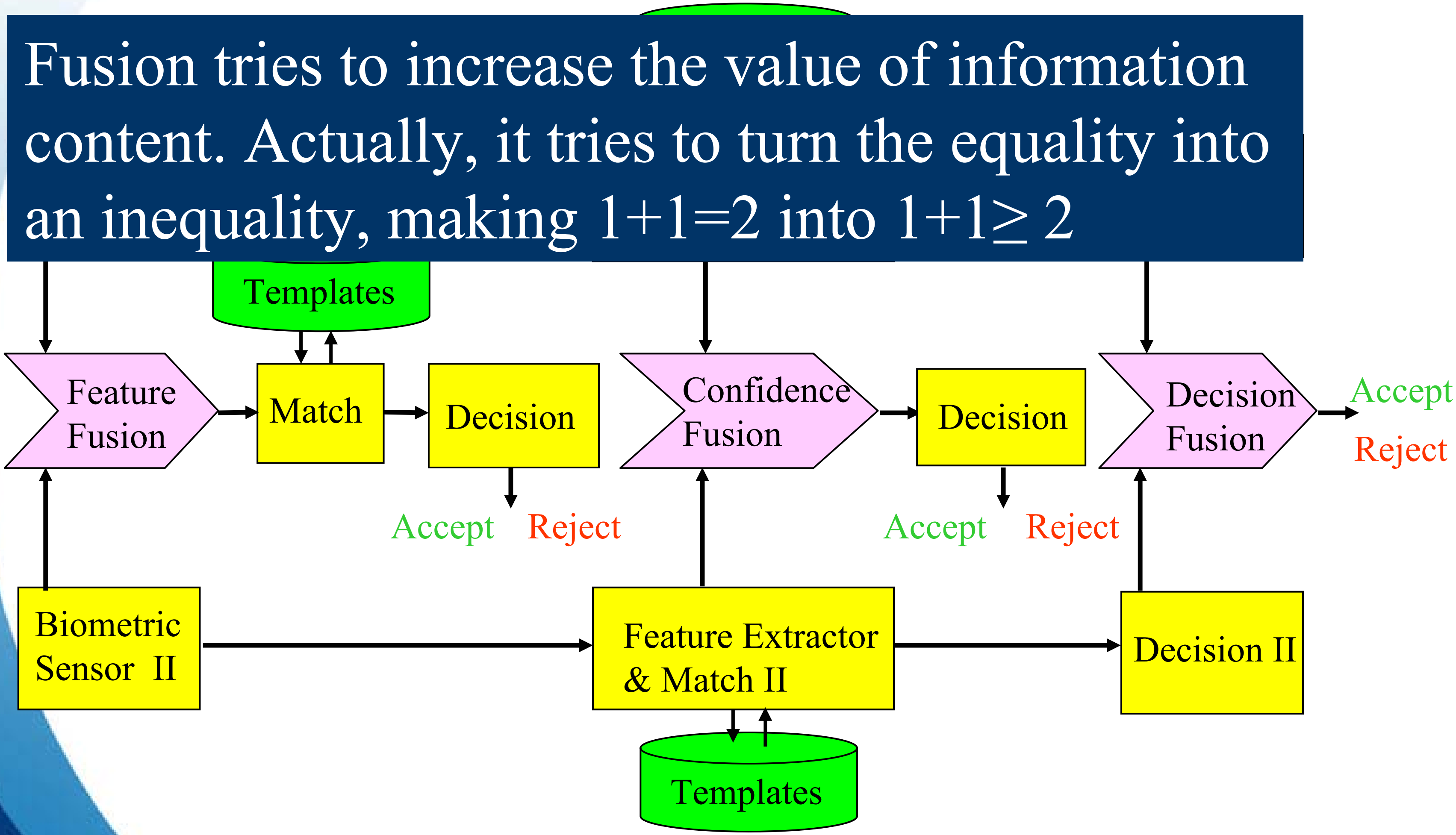
- Biometric Fusion Demo System
  - Different fingerprint sensors
  - Different biometric technologies
- Research on Multi-Modal Biometric Fusion
  - Fusion of independent modalities
  - Fusion of associated modalities

Biometric Fusion Demo System



Multi-Modal Biometric Fusion

Fusion tries to increase the value of information content. Actually, it tries to turn the equality into an inequality, making 1+1=2 into 1+1≥ 2

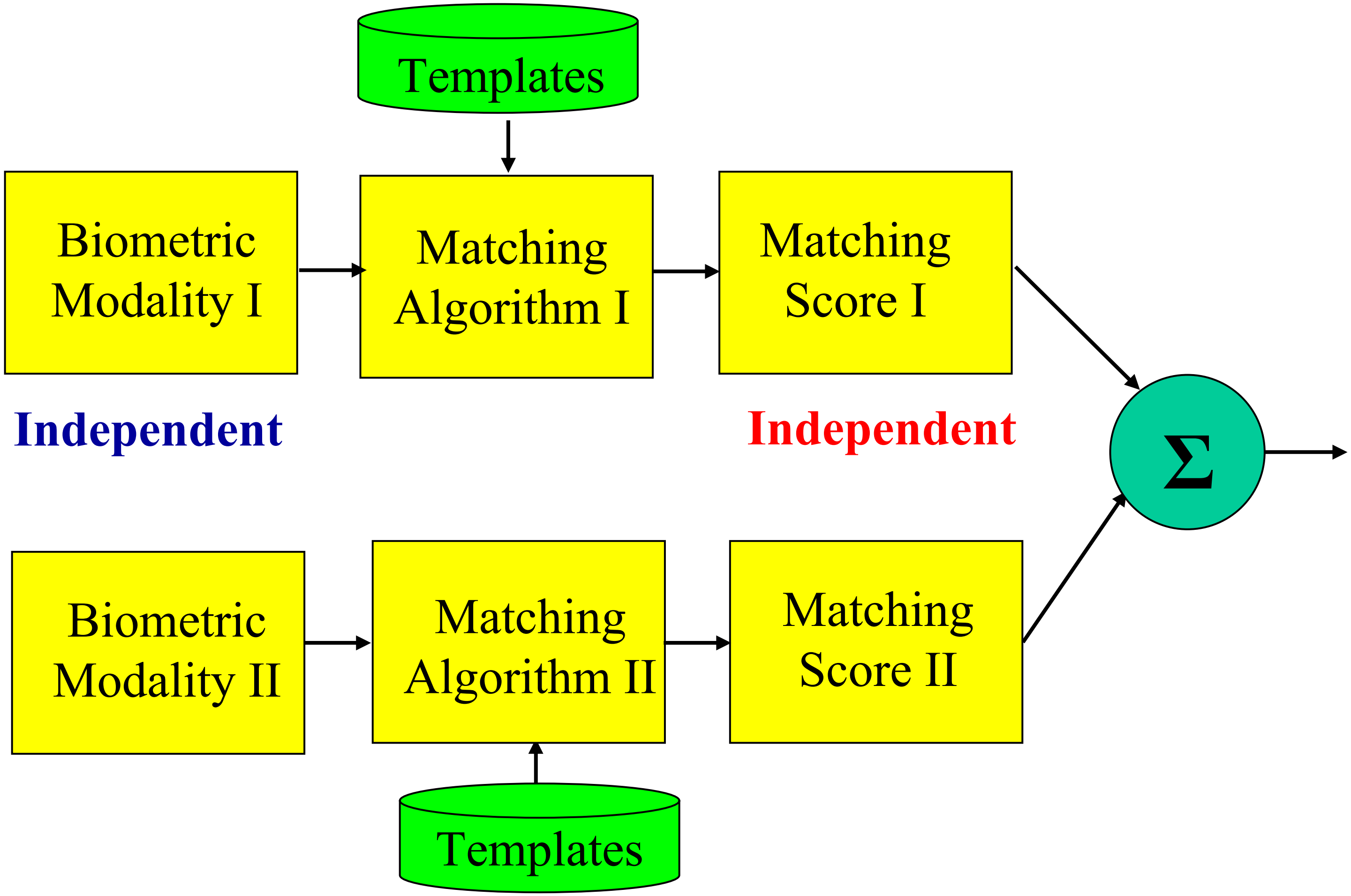


Reference [2]

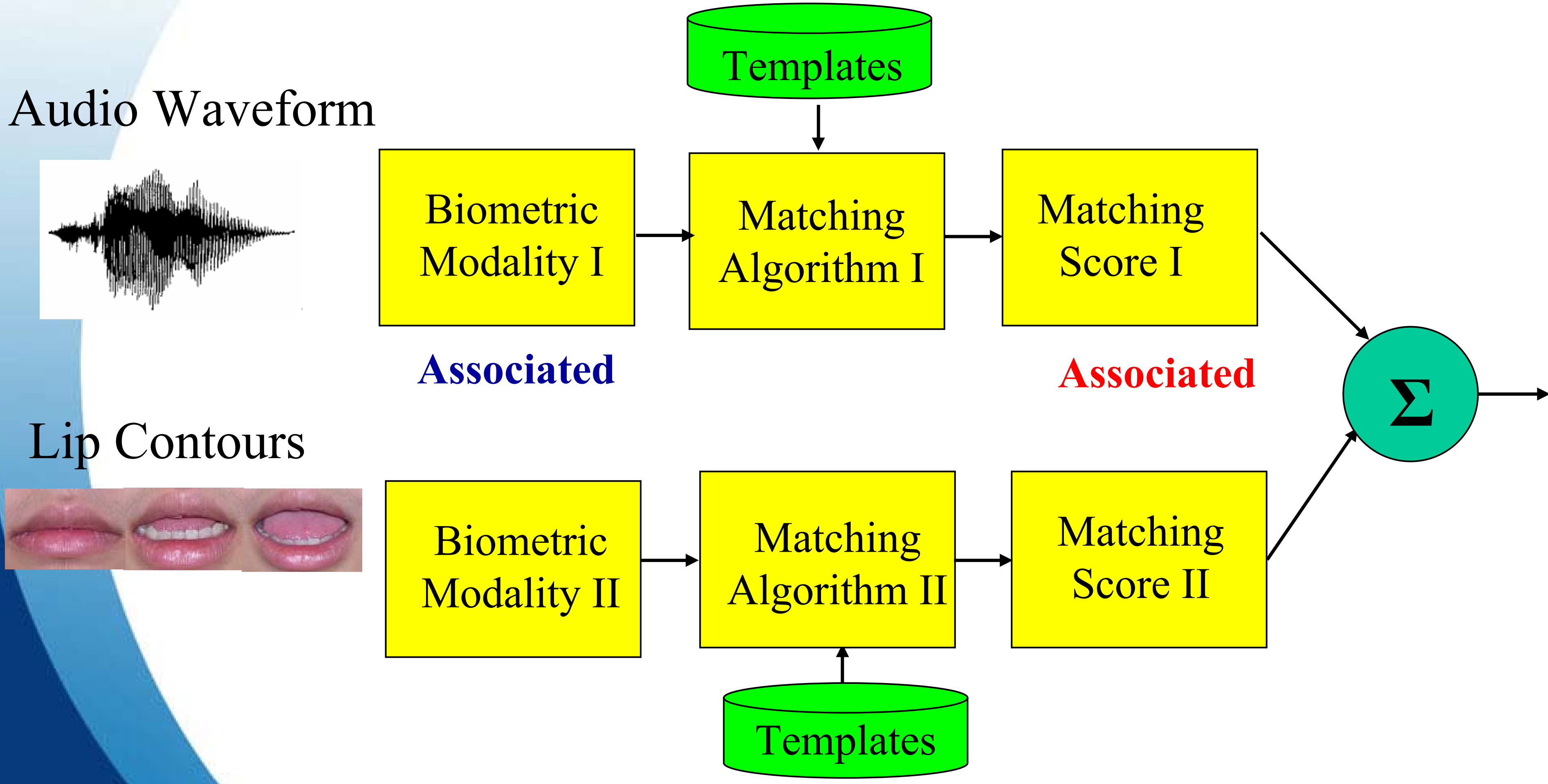
Independent Inputs

Fingerprint

Face Image



Associated (Dependent) Inputs



Audio Waveform

Lip Contours

Templates

Biometric Modality I

Matching Algorithm I

Matching Score I

Associated

Associated

Σ

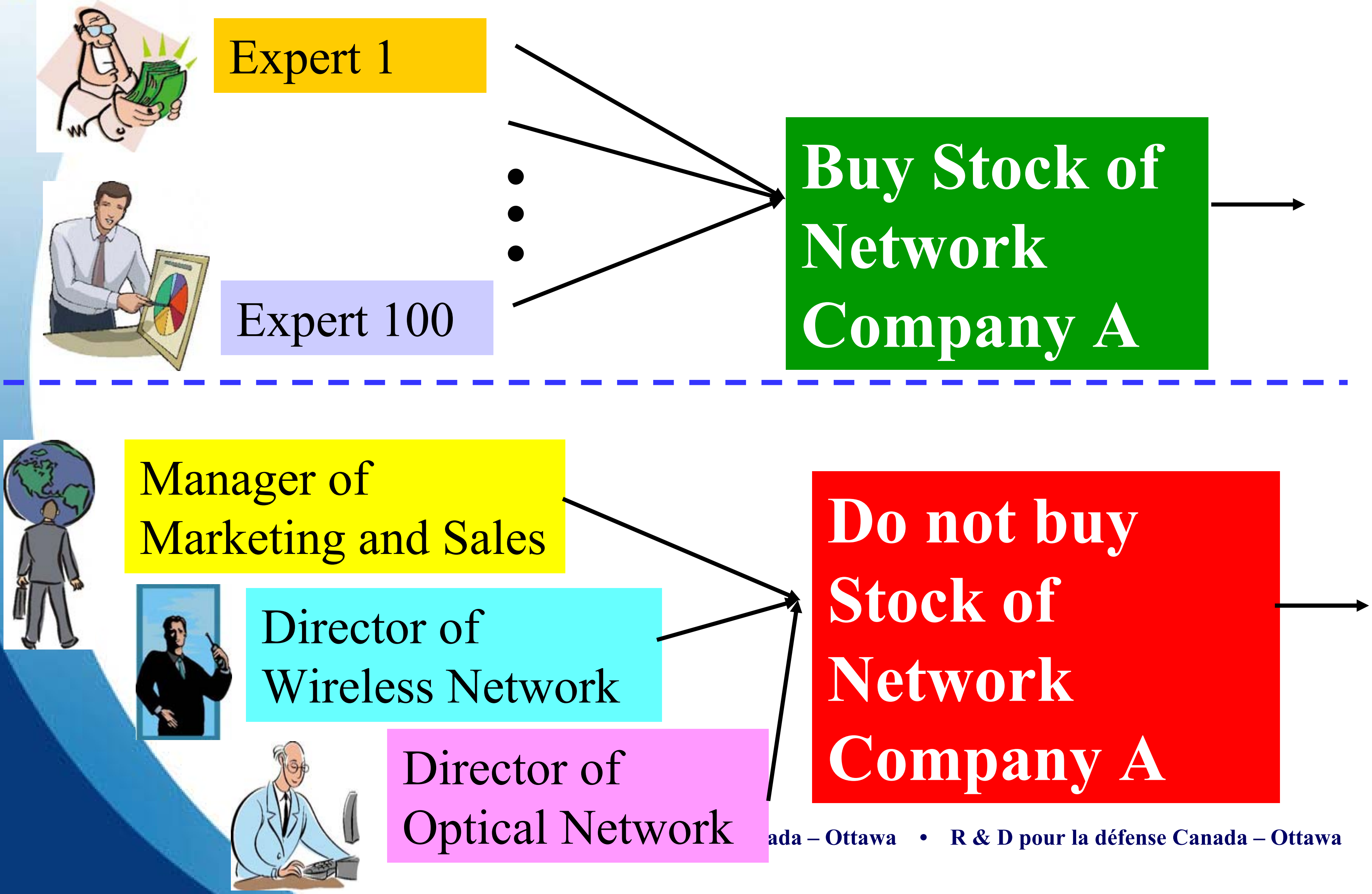
Biometric Modality II

Matching Algorithm II

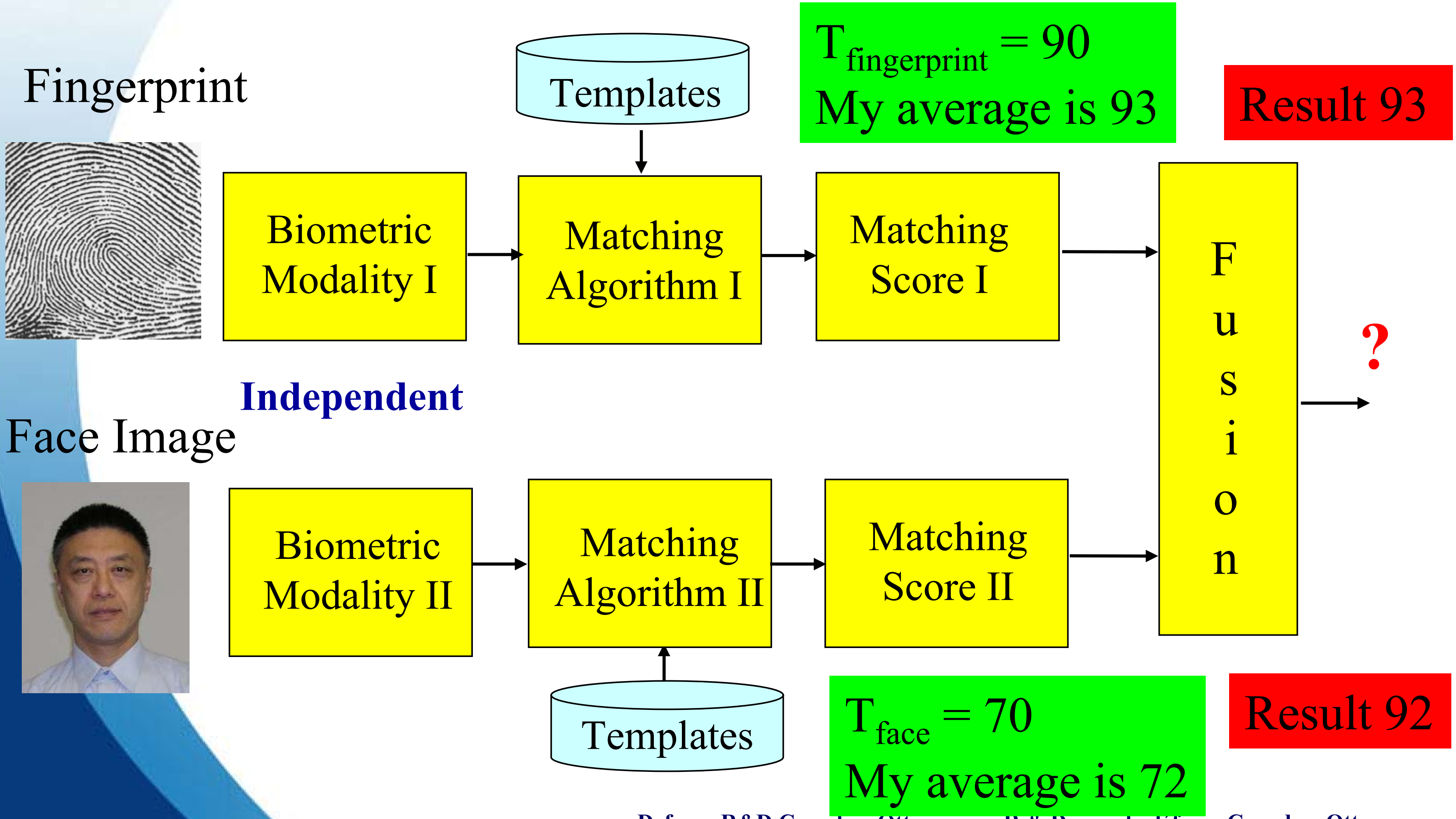
Matching Score II

Templates

Decision Making Based on Dependent vs. Independent Information


Expert 1
•
•
•
Expert 100
Buy Stock of Network Company A
Manager of Marketing and Sales
Director of Wireless Network
Director of Optical Network
Do not buy Stock of Network Company A

Is It Me?
— based on independent modalities



Fingerprint

Templates

Biometric Modality I → Matching Algorithm I → Matching Score I

$T_{fingerprint} = 90$
My average is 93

Result 93

Independent

Face Image

Biometric Modality II → Matching Algorithm II → Matching Score II

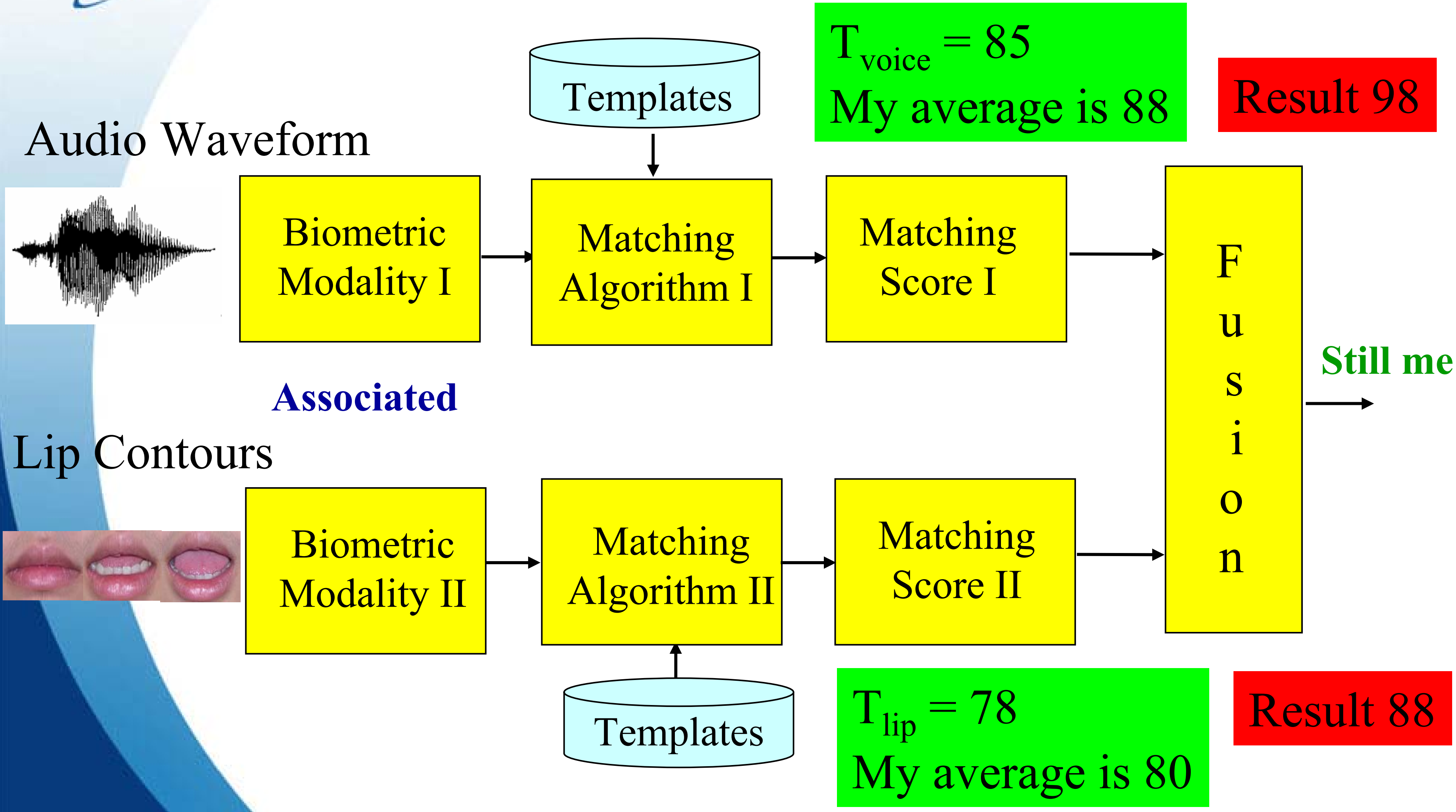
Templates

$T_{face} = 70$
My average is 72

Result 92

Fusion → ?

It is Still Me!
— based on associated modalities



Audio Waveform

Biometric Modality I

Templates

Matching Algorithm I

Matching Score I

T_{voice} = 85
My average is 88

Result 98

Associated

Lip Contours

Biometric Modality II

Matching Algorithm II

Templates

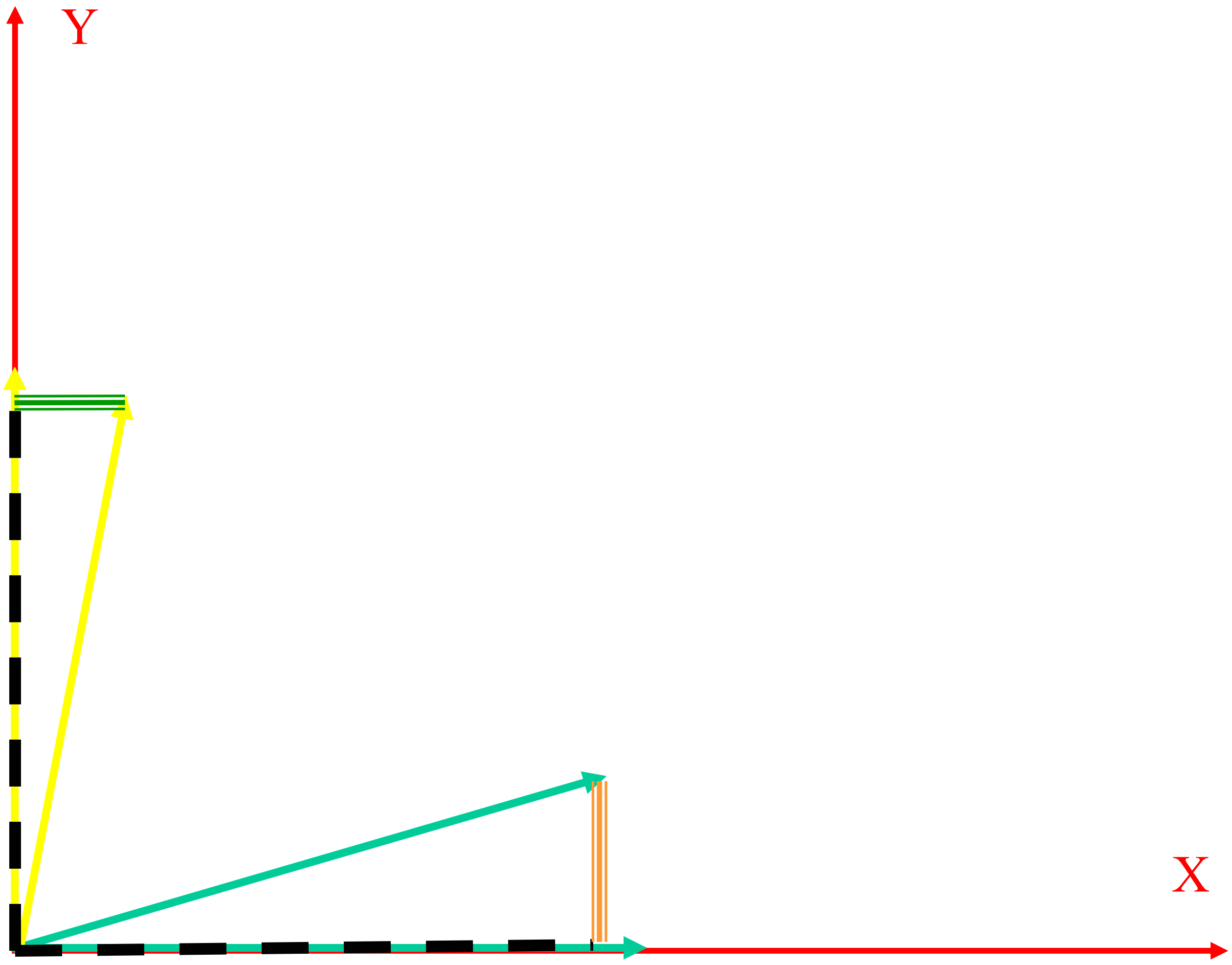
Matching Score II

T_{lip} = 78
My average is 80

Result 88

Fusion

Still me


Y
X

Conclusion

- Using biometrics can enhance the security level of e-authentication
- Spoofing is a major vulnerability
- Several anti-spoofing technologies are under development
- Multi-modal biometric fusion is a potential solution
- Fusion on associated biometric modalities might be a better solution because the sensor fusion can be performed with rich information obtained at an early stage

Acknowledgement

The author would like to thank Dr. Mark McIntyre and Dr. Karim Dahel for their comments and suggestions, and Mr. Matthew Kellett for his careful corrections and editing.

References

[1] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, “Impact of artificial gummy fingers on fingerprint systems,” *Proc. of SPIE Vol. #4677*, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

[2] A. Ross, A. K. Jain, and J. Qian, “Information fusion in biometrics,” in *Proc. AVBPA’01*, Halmstad, Sweden, pp. 354-359, June 2001.

DEFENCE R&D DÉFENSE